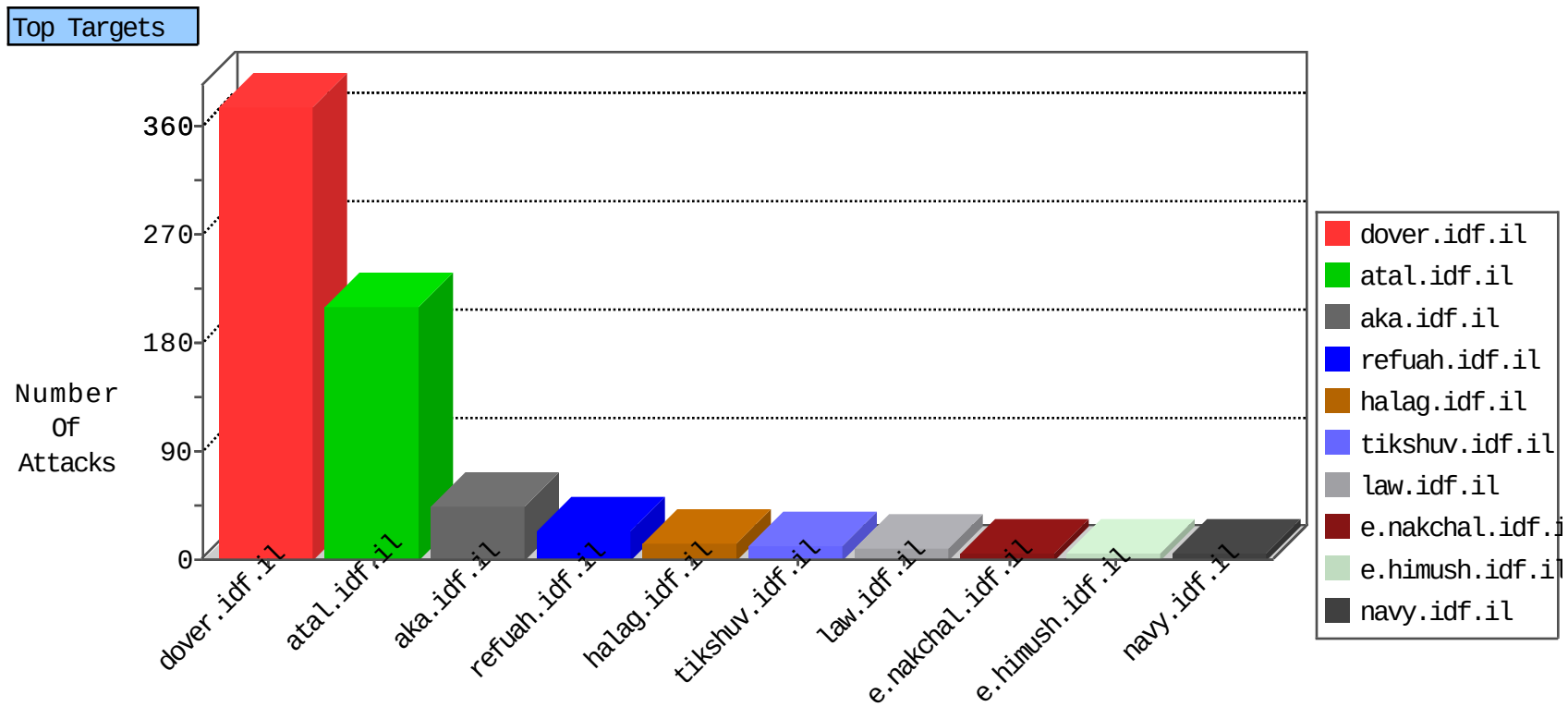
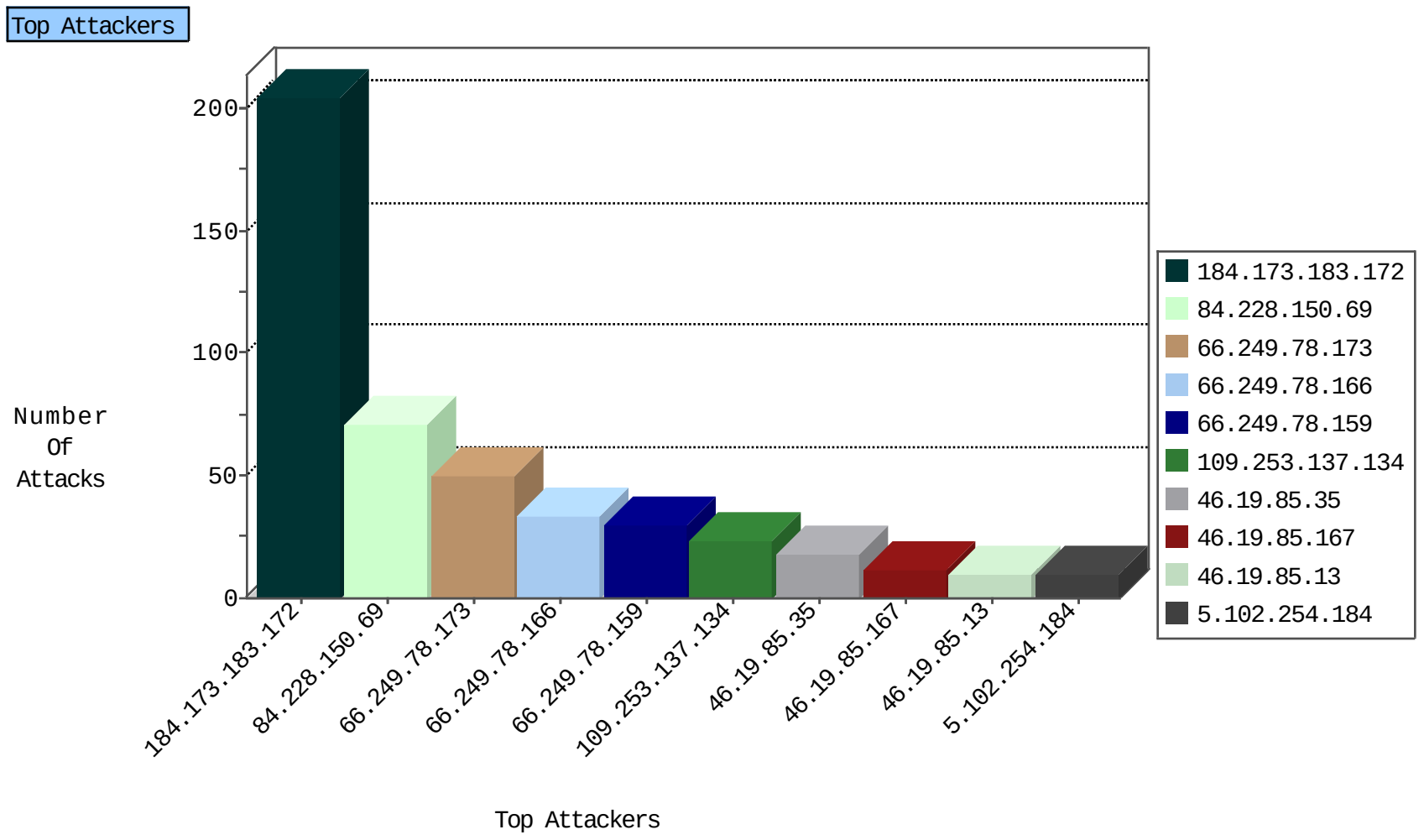
05-03-2015-02:03:02 to 05-03-2015-03:03:02

IDF Under Attack
05-03-2015-02:03:02

Top Targets



Top Attackers



05-03-2015-02:03:02 to 05-03-2015-03:03:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Web Site	Signature	Device Action	Count
220.181.108.95	China	147.237.76.42	refuah.idf.il	TCP handshake violation, first packet not syn	drop	150
82.80.25.221	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	4
10.0.0.21		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
71.6.135.131	United States	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
5.102.254.135	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1

05-03-2015-02:03:02 to 05-03-2015-03:03:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
184.173.183.172	United States	147.237.77.233	atal.idf.il	DVRep_P-N_40-59	Permit	205
109.64.14.34	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
71.6.167.142	United States	147.237.76.196	e.sviva.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.86	navy.idf.il	DVRep_B-N_60_100	Block	1
46.116.202.157	Israel	147.237.77.216	dover.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.76.38	e.e.meitav.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.16	my-kosher-kravi.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.72.217	e.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.202	e.halag.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.77.61	e.cogat.idf.il	DVRep_B-N_60_100	Block	1
66.240.192.138	United States	147.237.8.45	e.eitan.idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.76.199	e.nakchal.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
194.247.12.82	Ukraine	147.237.76.39	mobile.meitav.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
71.6.167.142	United States	147.237.77.176	matpash.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.76.31	nakchal.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.33	idf.il	DVRep_B-N_60_100	Block	1
85.25.103.50	Germany	147.237.77.216	dover.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.8.50	e.tikshuv.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
85.25.43.94	Germany	147.237.0.35	akaws.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.170	maarachot.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.34	tikshuv.idf.il	DVRep_B-N_60_100	Block	1
93.120.27.62	Romania	147.237.76.177	ncore.idf.il	DVRep_B-N_60_100	Block	1
71.6.167.142	United States	147.237.76.34	yohalan.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.76.39	mobile.meitav.idf.il	DVRep_B-N_60_100	Block	1
5.102.254.184	Israel	147.237.72.166	aka.idf.il	7120: TCP: Segment Overlap With Different Data, e.g., Fragroute	Block	1
85.25.103.50	Germany	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1
71.6.165.200	United States	147.237.77.235	sviva.idf.il	DVRep_B-N_60_100	Block	1
66.240.236.119	United States	147.237.0.200	m4u.idf.il	DVRep_B-N_60_100	Block	1

05-03-2015-02:03:02 to 05-03-2015-03:03:02

Top Attackers In IDS

Attacker Address	Attacker Country	Target Address	Site	Name	Count
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Tehila - Perl LWP with fake user agent	6
66.249.69.66	United States	147.237.77.233	atal.idf.il	ET SCAN NMAP -sA (2)	2
66.249.67.34	United States	147.237.77.226	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	2
61.240.144.64	China	147.237.0.35	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.76.42	refuah.idf.il	ET SCAN Potential SSH Scan	1
12.139.34.20	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 2048	1
199.255.137.52	United States	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
199.255.137.52	United States	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -f -sS	1
193.107.17.72	Russian Federation	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
183.232.128.156	China	147.237.0.34	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
61.240.144.66	China	147.237.76.42	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.76.39	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
218.77.79.43	China	147.237.77.178	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
12.139.34.20	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -sS window 4096	1
218.77.79.43	China	147.237.0.19	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
12.139.34.20	United States	147.237.77.74	law.idf.il	ET SCAN NMAP -f -sS	1
199.255.137.52	United States	147.237.76.199	e.nakchal.idf.il	ET SCAN NMAP -sS window 2048	1
193.107.17.72	Russian Federation	147.237.76.199	e.nakchal.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
178.32.251.100	France	147.237.77.227	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	China	147.237.77.212	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1

05-03-2015-02:03:02 to 05-03-2015-03:03:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Message	Name	Device Action	Count
84.228.150.69	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	71
66.249.78.173	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	46
66.249.78.166	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	28
66.249.78.159	United States	147.237.77.216	dover.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	26
109.253.137.134	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	23
46.19.85.35	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	14
46.19.85.13	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	10
37.48.120.214	Netherlands	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	8
46.19.85.167	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	7
192.117.118.5	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
46.19.85.93	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	7
5.102.254.184	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	6
66.249.78.44	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
31.210.186.177	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
66.249.78.51	United States	147.237.77.234	halag.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	6
166.137.118.107	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
41.33.231.86	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	6
46.19.86.150	Israel	147.237.76.42	refuah.idf.il	Invalid ACK number	Bad TCP sequence	monitor	5
157.55.39.191	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	5
157.55.39.204	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
217.83.85.203	Germany	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.19.85.35	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
37.18.51.54	Russian Federation	147.237.76.197	e.himush.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	4
5.102.254.135	Israel	147.237.77.216	dover.idf.il	Invalid ACK number	Bad TCP sequence	monitor	4
157.55.39.138	United States	147.237.72.166	aka.idf.il	Invalid segment retransmission. Packet dropped.	Streaming Engine: TCP Invalid Retransmission	drop	4
2.52.46.121	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
46.19.85.167	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	4
50.190.212.149	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
195.34.150.18	Austria	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
94.230.86.169	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	monitor	3
41.42.104.241	Egypt	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
186.249.49.57	Brazil	147.237.77.121	e.navy.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	3
109.67.176.113	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	3
5.102.254.184	Israel	147.237.72.166	aka.idf.il	Invalid ACK number	Bad TCP sequence	alert	3
94.253.139.114	Croatia	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
2.220.98.131	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
87.68.20.227	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
37.140.141.39	Russian Federation	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
68.180.228.117	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
54.72.0.55	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
82.28.126.11	United Kingdom	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
192.249.64.249	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
8.37.227.69	Anonymous Proxy	147.237.77.216	dover.idf.il	Response out of state	Block HTTP Non Compliant	monitor	2
54.72.73.168	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
50.87.144.145	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
79.179.176.113	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
61.135.190.197	China	147.237.0.200	m4u.idf.il	Geo-location inbound enforcement	Geo-location enforcement	drop	2
37.46.39.22	Israel	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2
209.133.111.211	United States	147.237.77.216	dover.idf.il	First packet isn't SYN	drop	drop	2

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Name	Device Action	Count
66.249.78.173	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.173	Block	4
66.249.78.166	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.166	Block	4
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	3
207.46.13.101	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
157.55.39.137	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
157.55.39.138	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
79.179.35.96	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il//main/haredim/webresource.axd	Block	1
188.165.15.195	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/french/main.stm	Block	1
66.249.75.65	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/938-he/atal.aspx	Block	1
66.249.64.240	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-13112-he/dover.aspx	Block	1
157.55.39.192	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.192	Block	1
157.55.39.53	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il//captcha.ashx	Block	1
207.46.13.109	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/shared/usercontrols/headerupper/	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/french/idf_in_pictures/2003/june/16d.stm	Block	1
66.249.75.26	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
157.55.39.138	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.138	Block	1
50.28.33.173	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/test/wp-admin/	Block	1
80.169.156.100	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/console/core/doc_mgr/mce_src=	Block	1
190.185.229.232	Argentina	147.237.77.74	law.idf.il	Distributed Unknown HTTP Request Method	Block	1
66.249.78.51	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/mobile/	Block	1
66.249.67.6	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed Unauthorized URL Access on 147.237.77.226//938-he/hamaz.aspx	Block	1
157.55.39.192	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nahal	Block	1
157.55.39.61	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
68.180.228.117	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/0102-2.stm	Block	1
208.113.186.110	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wp-admin/	Block	1
180.76.4.27	China	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
66.249.75.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/sachar/faq.aspx	Block	1
157.55.39.161	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/110-he/patzar.aspx	Block	1
50.62.57.239	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/blog/wp-admin/	Block	1
91.216.107.204	France	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wordpress/wp-admin/	Block	1
207.46.13.99	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il//captcha.ashx	Block	1
66.249.78.118	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/templates/getfile/getfile.aspx	Block	1
66.249.67.22	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/1120-he/hamaz.aspx	Block	1
157.55.39.204	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/main.asp	Block	1
210.172.144.87	Japan	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/wp/wp-admin/	Block	1
188.138.17.205	France	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on 147.237.76.31//	Block	1
66.249.75.42	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
157.55.39.162	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/443-he/patzar.aspx	Block	1
61.135.190.69	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/	Block	1
93.148.233.205	Italy	147.237.77.176	matpash.idf.il	Unknown HTTP Request Method COOK in URL www.cogat.idf.il/894-en/matpash.aspx	Block	1
66.249.67.59	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/1116-he/nakhal.aspx	Block	1
178.90.161.11	Kazakstan	147.237.77.74	law.idf.il	Unknown HTTP Request Method COOK in URL www.law.idf.il/163-7225-en/patzar.aspx	Block	1
157.55.39.137	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.137	Block	1
37.23.102.164	Russian Federation	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/console/core/doc_mgr/doc_mgr.asp	Block	1
78.183.32.126	Turkey	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
188.165.15.41	France	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/shared/usercontrols/headerupper/	Block	1
66.249.75.49	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1242-he/atal.aspx	Block	1
157.55.39.191	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/site/news.aspx	Block	1
66.249.64.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.74	Block	1

05-03-2015-02:03:02 to 05-03-2015-03:03:02